REMARKS

Claims 1, 3-5, 7-20, 22-31 and 33-37 are amended, Claim 2 is canceled and Claims

38-41 are added. Accordingly, Claims 1 and 3-41 are pending in the application. In view of

the following remarks, Applicants respectfully request reconsideration and allowance of the

subject application.

Rejection under 35 U.S.C. § 102

Claims 1-37 stand rejected under 35 U.S.C. § 102 as being anticipated by Oaks.

Applicants respectfully traverse the rejection of Claims 1-37. Before undertaking a

discussion of the substance of the Office's rejection, the following discussion of Applicants'

disclosure and the reference Oaks is provided in an attempt to assist the Office in

appreciating certain distinctions between the claimed subject matter and Oaks.

Applicants' Disclosure

As described in the present Application, a permission set and a set of requestable

permissions associated with a code assembly are received. A grantable permission set is

generated from the subset of the permission set specified by the set of requestable

permissions. Upon receipt of a request for permission to access a resource, the grantable

permission set is utilized to determine if the access to the resource should be granted or

denied. Neither the set of requestable permissions nor the grantable permission set constitute

the actual request for permission to access a resource, nor the actual granting or denial of the

access to the resource.

The Oaks Reference

By contrast, Oaks discloses that an access controller enforces an access policy specified in a file. Oaks defines an access policy as an encapsulation of all the specific permissions that should be granted to specific code sources. Oaks defines a permission as an encapsulation of a request to perform a particular operation. Oaks further defines a protection domain as an encapsulation of a particular code source and the permission granted to the specific code source. Accordingly, upon receipt of a permission to access a resource, the policy is utilized to determine if access to the resource should be granted or denied.

The Claim Rejection

Claim 1 recites a method for processing a permission set associated with a code assembly received from a resource location to control execution of the code assembly. The method, as amended, comprising:

receiving the permission set including at least one permission associated with the code assembly;

receiving a set of requestable permissions association with the code assembly; and

generating a grantable permission set from a subset of the permission set specified by the set of requestable permissions, prior to execution of the code assembly.

Applicants respectfully assert that Oaks fails to disclose the method of Claim 1. Oaks only discloses receiving a permission and granting a protection domain in accordance with a

received security policy. The security policy, as disclosed in Oaks, is an encapsulation of the specific permissions that should be granted to a specific code source. Oaks does not disclose "receiving a set of requestable permissions associated with the code assembly." The rejection incorrectly associates the set of requestable permissions with an actual request for permission generated during execution of the code. The set of requestable permissions are not equivalent to the actual requests for permissions made during execution of the code. Applicants have amended the limitation "permission request set" to "set of requestable permissions" to clarify that a set of permissions that are requestable by the code assembly are received, instead of receipt of a specific run-time requests for permission.

In addition, Oaks does not disclose generating a grantable permission set from a subset of the permission set specified by the set of requestable permissions. The rejection incorrectly associates the grantable set of permissions with an actual granted permission generated during execution of the code. Applicants have amended the limitation "permission grant set" to "set of grantable permissions" to clarify that a set of permissions that are grantable are generated, instead of the actual grant of permissions during runt-time. For these reasons, Claim 1 is allowable over Oaks. Applicants therefore respectfully request that the §102(b) rejection of Claim 1 be withdrawn.

Dependent Claims 2-19 are also allowable by virtue of their dependency on respective base Claim 1, as well as the additional elements they recite. With regard to Claim 4, Oaks does not disclose a set of requestable permissions, nor that the set of requestable permissions specifies a minimum permission condition. Accordingly, Oaks does not disclose

"comparing the permission set and a minimum permission condition specified by the set of requestable permissions" or "preventing loading of the code assembly, if the permission set fails to satisfy the minimum permission condition." Instead, Oaks discloses actually granting or denying a permission based upon a received security policy.

With regard to Claim 5, Oaks does not disclose a set of requestable permissions, nor that the set of requestable permissions specifies a minimum permission condition. Accordingly, Oaks does not disclose "preventing execution of the code assembly, if the permission set fails to satisfy a minimum permission condition specified by the set of requestable permissions." Instead, Oaks discloses actually granting or denying a permission based upon a received security policy.

With regard to Claim 12, Oaks does not disclose that "the set of requestable permissions specifies an optional set of permissions requested in association with the code assembly," wherein the optional set of permission pertain to a single code assembly. Instead, Oaks discloses that a first code may be trusted and therefore be permitted to perform any operation and that a second code may be untrusted and therefore be subject to the full extent of the security policy enforced by the security manager.

With regard to Claim 13, Oaks does not disclose that "the set of requestable permissions specifies an optional set of permissions requested in association with the code assembly." Thus, Oaks also does not disclose "executing a first level of code assembly functionality if a first optional set of permissions specified in the requestable permission set

is a subset of the permission set" and "executing a second level of code assembly functionality if a second optional set of permission specified in the requestable permission set is a subset of the permission set." Instead, Oaks only discloses actually granting or denying a permission based upon a received security policy. For the above-advanced reasons, Applicants assert that Claims 2-19 are patentably distinguishable over Oaks. Accordingly, Applicants respectfully request that the §102(b) rejection of Claims 2-19 be withdrawn.

Claims 20, 33, 34 and 35 are rejected for the same reasons as Claim 1. To the extent that Claims 20, 33, 34 and 35 are similar to Claim 1, Applicants respectfully assert that Claims 20, 33, 34 and 35 are allowable over Oaks for the same reasons advanced in support of Claim 1. Dependent Claims 21-32, 36 and 37 are allowable by virtue of their dependency on respective base Claims 20, 33, 34 and 35, as well as the additional elements they recite. Accordingly Applicants respectfully request that the §102(b) rejection of Claims 20-37 be withdrawn
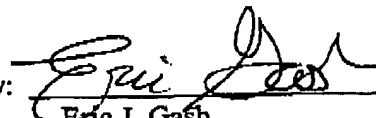
New Claims 38-41 are provided for examination. Applicant believes that these claims are allowable over the prior art of record.

Conclusion

Claims 1 and 3-41 are in condition for allowance. Applicant respectfully requests prompt allowance of the subject application. If any issue remains unresolved that would prevent allowance of this case, the Examiner is requested to contact the undersigned attorney to resolve the issue.

Respectfully Submitted,

Date: _5/12/05_

By: _Eric J. Gash_
Lee & Hayes, PLLC
Reg. No. 46,274
(509) 324-9256 ext. 228